



# The Muslim Co-operative Bank Ltd.

## ATM Policy

### DOCUMENT CONTROL

Reference Number	Version	Approval Date	Document Classification
PL-29	1.0	18/10/2022	1. Yearly Review.

---

**Table of contents**

<b>1. PURPOSE.....</b>	<b>4</b>
<b>2. OBJECTIVE.....</b>	<b>4</b>
<b>3. SCOPE .....</b>	<b>4</b>
<b>4. OVERSIGHT AND PUBLIC POLICY GOALS .....</b>	<b>5</b>
<b>5. MANAGEMENT RISK ANALYSIS:.....</b>	<b>5</b>
<b>6. ATM RISK MANAGEMENT:.....</b>	<b>5</b>
<b>7. TYPES OF ERRORS .....</b>	<b>6</b>
<b>8. ATM TECHNOLOGICAL STANDARDS AND SECURITY MEASURES:....</b>	<b>8</b>
<b>9. SECURITY AND CONTROL OF PIN (PERSONAL IDENTIFICATION NUMBER) .....</b>	<b>9</b>
<b>10. APPLICATION CONTROL AND SECURITY:.....</b>	<b>10</b>
<b>11. GENERAL INFORMATION REGARDING DELIVERY CHANNELS .</b>	<b>12</b>
<b>12. CUSTOMER AWARENESS ON FRAUDS.....</b>	<b>13</b>
<b>13. EMPLOYEE AWARENESS AND TRAINING .....</b>	<b>14</b>
<b>14. THREATS TO ATM NETWORKS .....</b>	<b>14</b>
<b>15. ATM INCIDENT MANAGEMENT POLICY AND PROCEDURES....</b>	<b>18</b>
<b>16. ATM CUM DEBIT CARD ACCEPTANCE OF USE POLICY .....</b>	<b>23</b>

17. **FAQS FOR ATM DEBIT/CREDIT CARDS .....33**

18. **ROLES AND RESPONSIBILITIES .....39**

19. **INQUIRIES .....39**

20. **AMENDMENTS (REVISION HISTORY).....39**

21. **DOCUMENT HISTORY .....39**

---

## 1. PURPOSE

- The Muslim Co-operative Bank Ltd. MCOB was founded in 1931 is serving for its customers on various channels. Being top bank in Co-Operative section, bank is providing its customers advance services and features.
- In the age of electronic and mobile devices banking sector has shown a tremendous growth. bank has also taken various initiatives in order to keep in competition with growing banks.
- Today, almost every commercial bank branch is at some stage of technology adoption: Core banking solution (CBS) or alternate delivery channels such as internet banking, mobile banking, phone banking and ATMs. Hence with emerging technology there arises a need of security, in terms of finance, data and other aspects of information.
- The Muslim Co-operative Bank Ltd. has introduces 19000 ATM Card.The Application service provider is Sarvatra pvt ltd Pune.The Switch services and Support of services are included in the ASP agreement.

## 2. OBJECTIVE

- To achieve safe, sound and resilient ATM network and cash flow bidding with the technological standards mentioned as per RBI and IT ACT 2000 and IT Amendment Act and other governing laws.
- This document identifies security guidelines for ATMs, considering the protection that can be provided by the hardware and the software of the ATM itself against attacks aimed at compromising sensitive data acquired, stored, exported, or in any way processed by the device.
- The Policy is formulated for the IT department and ASP Provider or the Banking cell taking in or working for the ATM related services

## 3. SCOPE

- This policy document covers the implementation of new features, operations, roles and responsibilities in ATM channel and services.

---

## 4. OVERSIGHT AND PUBLIC POLICY GOALS

- The Bank monitors and review ATM services from time to time and ensure that:
  1. The legal and regulatory environment is appropriate and keeps pace with domestic Developments.
  2. International standards are complied with in respect of infrastructures and cards to Reduce risk and increase safety and efficiency.
  3. The provision of services by the Head Office is fair and based on objective criteria.

## 5. MANAGEMENT RISK ANALYSIS:

- Bank has been following and implemented the process of identifying, measuring, monitoring and managing all potential risk in ATM transactions.
- Bank is identifying, monitoring and keep track report of the following on regular basis.
  - I. Total no. of active ATMs
  - II. Time Logged on/ Settlement time.
  - III. Number of Cardholders.
  - IV. Number of transactions i.e. withdrawals and transfers
  - V. Total amount transacted through withdrawals and transfers.
  - VI. ATM internal process and services.
  - VII. Operations of ATM channel.
  - VIII. Legal Risk.
  - IX. Incident Management.
  - X. Risk Management.

## 6. ATM RISK MANAGEMENT:

BANK would review the risk and monitor ATM services by following below mentioned Aspects:

- Monitoring and checking that all ATM should be equipped with mechanism preventing Skimming attacks,
- Applied mechanism to monitor that each ATM is equipped with only one card holder Interface,

- 
- Continues surveillance on all ATM that they are equipped with security Cameras,
  - Take all necessary steps to protect ATM assets and Application,
  - Managing and identifying various hazards to which ATM centres that may exposed Including natural disaster or otherwise,
  - Identifying the controls that are in operation to reduce possible impacts of Threats/risks,
  - Following all the security controls and guidelines suggested by PCI DSS,
  - Firewall should be configured and be kept up to date and should allow only known Application traffic inward and outward,
  - Patch management program for ATM operating system and applications should be in Place to ensure ATM software is well patched,
  - Software White listing solution for ATMs and it should be in place and an anti-virus Must be installed and always updated,
  - Develop an incident management system and an incident response plan prepared for
  - Rapid deployment in case of a compromise. This is to ensure ATM frauds are reported in real time,
  - ATM software must be updated regularly,
  - ATM operators should migrate to EMV chip and pin card and should eliminate Magnetic stripe fall back. This will mitigate the risk of skimming cards,
  - Segregation of ATM network from the rest of the bank's network by using a firewall and virtual local area networks,
  - ATM PC BIOS must be secured,
  - A password policy must be in place to ensure only strong passwords are used on ATMs and each user has their own unique password,
  - All communications on the ATMs that is encrypted including communication between the PC core and the cash dispenser,
  - All unused services and applications must be removed from the ATM to reduce the attack surface,
  - Ensuring ATM physical security like CCTV and alarms when installing the ATM.

## 7. TYPES OF ERRORS

Bank have management/handling plan for the following errors can occur due to Mechanical failure at the ATM terminal:

- I. ATM dispenses less cash to the customer but the amount is debited correctly
- II. The customer's account is debited twice but the cash is only dispensed once by ATM
- III. The Customer's account is debited but cash is not dispensed by ATM

---

## ATM SECURITY MEASURES:

### The ATM Audit Log

Record and track of ATM audit Log that provides recorded information after incident.

- **Encryption**

All ATM system installed are encrypted and updated time to time.

- **Software Audit**

Perform software audit of all installed and active ATMs to analyse the ATM operations. Monitoring operations of ATMs and detect possible tampering with the programs. Perform audit to detect that program are being properly executed and not being over-ridden or bypassed.

- **CONTROLS**

This requirement should be addressed with the controls implemented at different levels of ATM implementation, such as General Application Control, Business Process Control, and Application Process Control, CIA Controls.

- **General ATM operation and Organizational Controls:**

The operation and organizational controls must be segregated among the individuals, There are two main important elements in an ATM systems; firstly the magnetic card and secondly PINs. Segregation of duties shall be maintained by assuring that making of the PINs is not to be carried out by people who are processing the cards.

### Following segregation is to be followed by Bank:

- Application testing from systems design and programming
- System software programming from Application programming
- The total ATM withdrawal limit is set as per bank limit. (Limit is subject to change time to time as per requirement or the limit decided by the NPCI)
- The Password of the cash vault must change every 15 days
- The ATM cards above 30 days, when the card first received by the Branch should be disabled and destroyed
- The 3 ATM keys should be maintained by Cashier, Passing Officer and the Authority at Head Office respectively.
- If the Cashier or Passing officer is transferred / deputed then the Vault password must be changed and kept confidential.
- The record of the changed passwords should be maintained and updated time to time.

- Cash filled in ATM should be strictly under **banks cash policy**.

### **Business Process Controls**

Bank personnel having access to cards must be denied access to PINs whenever the cards are prepared and processed. Bank takes care of segregation of duties that no one person shall handle all the transaction. Bank makes sure that.

## **8. ATM TECHNOLOGICAL STANDARDS AND SECURITY MEASURES:**

Bank has established secured network and implemented security measures for mitigating risk in ATM operations, which are listed as below:

- a) All ATMs shall be operated for cash replenishment only with digital One Time Combination (OTC) locks.
- b) All ATMs shall be grouted to a structure (wall, pillar, floor, etc.), except for ATMs installed in highly secured premises such as airports, etc. which have adequate CCTV coverage and are guarded by state / central security personnel.
- c) Bank also rolling out a comprehensive e-surveillance mechanism at the ATMs to ensure timely alerts and quick response.

- **Monitoring**

The following scope is inclusive of problem determination and resolution tasks which Bank is considering for central management of ATMs, all of which can be performed remotely with good ATM monitoring and management tools:

- a) Gracefully reboot the ATM; allow current transactions to finish before rebooting!
- b) Retrieve log files and security events.
- c) Retrieve performance information about memory, disk space, CPU usage, process lists, network ports, etc.
- d) Restart critical services on the ATM.

- **Integration**

Management and security tools that Bank has been used successfully in ATM systems which are mentioned below:

- Central authentication of user accounts used at the ATM.
- Inventory systems to track information about ATM hardware and software.
- Network monitoring systems to analyse the network performance of the ATMs.

- **Cryptographic Key Management for ATMs**

Bank applies key management process which is associated with financial transactions and for encrypting PIN Pad. The very essence of protection in an encrypted environment is the secrecy of the key.



- **Firewalls and Network Isolation**

Bank has installed software based firewall protection which has been the most security measure as it cannot be compromised through physical access alone. Bank has established effective network isolation and intrusion detection/ risk mitigation tools. Bank uses network isolation or network encryption techniques to ensure that cardholder data cannot travel outside the ATM system itself. Bank has a good core set of layered security which involves network isolation, tested operating system hardening, secure operating processes, and central monitoring/ management tools.

## **9. SECURITY AND CONTROL OF PIN (PERSONAL IDENTIFICATION NUMBER)**

PINs are stored in encrypted form and should be stored in database file for security purposes. The PIN mailers are prepared separately and also bank has taken necessary actions to check that PIN is not being misused by any Bank employee. Bank ensures that Pin is activated only upon the use of card by the customer at the ATM. For security and confidentiality reasons all systems documentation concerning PIN generation /encryption and decryption key must be under 3D level security controls all time.

- **Bank is implementing controls while providing ATM services are mentioned as below:**
  - I. PIN mailers should not have direct access to the customer's account number or any account related information.
  - II. Access controls and authorization to any addition, deletion or changes to ATM transaction details should be implemented
  - III. Any changes to cardholder details should be authorized by the officer at the next level.
  - IV. Realistic maximum transaction and maximum daily total limits should be implemented for ATM withdrawals.
  - V. Printed receipts should be dispensed by the ATM for every ATM transaction.
  - VI. out **Every ATM transaction should be acknowledged by e-mail or** short message script sent to the mobile phone to confirm or alert the user that a transaction was performed.

---

## 10. APPLICATION CONTROL AND SECURITY:

There are well-known information systems security issues associated with applications software, whether the software is developed internally or acquired from an external source. Attackers can potentially use many different paths through the application to do harm to the business. To determine the risk to itself, Bank has been evaluating the likelihood associated with the threat agent, attack vector and security weakness and combines it with an estimate of the technical and business impact to the organization. Together, these factors determine the overall risk.

The following are the important Application control and risk mitigation measures are implemented by Bank:

1. Each application has an owner which will typically be the concerned business function that uses the application

2. Some of the roles of application owners include:

- Prioritizing any changes to be made to the application and authorizing the changes
- Deciding on data classification /de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/ statutory requirements
- Ensuring that adequate controls are built into the application through active
- involvement in the application design, development, testing and change process
- Ensuring that the application meets the business/ functional needs of the users
- Ensuring that the information security function has reviewed the security of the application
- Taking decisions on any new applications to be acquired / developed or any old applications to be discarded
- Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements
- Ensuring that the Change Management process is followed for any changes in application
- Ensuring that the new applications being purchased/ developed follow the Information Security policy
- Ensuring that logs or audit trails, as required, are enabled and monitored for the applications
- All application systems are tested before implementation in a robust manner regarding controls to ensure that they satisfy business policies/rules of the bank and regulatory and legal prescriptions/requirements. Before the system is live, clarity on the audit trails and the specific fields that are required are captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.

- 
- Bank incorporates information security at all stages of software development. This would assist in improving software quality and minimizing exposure to vulnerabilities. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are required to be clearly specified at the initial stages of system development/acquisition. A compliance check against the bank's security standards and regulatory/statutory requirements is also done.
  - All application systems have audit trails along with policy/ procedure of log monitoring for such systems including the clear allocation of responsibility in this regard. Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, provides for detailed audit trails /logging capability with details like transaction id, date, time, originator id, authorizer id, actions undertaken by a given user id, etc. Other details like logging the IP address of the client machine, terminal identity or location may also be considered.
  - Applications also provide for, inter-alia; logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes, granting of access rights, use of system utilities, changes in system configuration, etc.
  - The audit trails are stored as per a **a \_ defined** period as per any Internal/regulatory/statutory requirements and it are ensured that they are not tampered with.
  - There are documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date.
  - The development, test and production environments are properly segregated.
  - Access is based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties is enforced.
  - There are controls on updating key 'static' business information like customer master files, parameter changes, etc.
  - Any changes to an application system/data are justified by genuine business need and approvals supported by documentation and subjected to a robust change management process. The change management would involve generating a request, risk assessment, authorization from an appropriate authority, implementation, testing and verification of the change done.
  - Potential security weaknesses / breaches (for example, as a result of analysing user behaviour or patterns of network traffic) are always identified.
  - There are appropriate measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.
  - Applications do not allow unauthorized entries to be updated in the database. Similarly, applications do not allow any modifications to be made after an entry is authorized. Any subsequent changes are made only by reversing the original authorized entry and passing a fresh entry.
-

- 
- Direct back-end updates to database not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.
  - Access to the database prompt is restricted only to the database administrator.
  - Robust input validation controls, processing and output controls are built in to the application.
  - Alerts regarding use of the same machine for both maker and checker transactions are considered.
  - Bank obtains application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/ modifications done).
  - For all critical applications, either the source code is received from the vendor or a software escrow agreement which is in place with a third party to ensure source code availability in the event the vendor goes out of business. It is ensured that product updates and programme fixes are also included in the escrow agreement.

Applications are configured to logout the users after a specific period of inactivity. The application ensures rollover of incomplete transactions and otherwise ensures integrity of data in case of a log out.

There are suitable interface controls in place. Data transfer from one process to another or from one application to another, particularly for critical systems, not has any manual intervention in order to prevent any unauthorized modification. The process are automated and properly integrated with due authentication mechanism and audit trails by enabling “Straight Through Processing” between applications or from data sources to replace any manual intervention/semi-automated processes like extracting data in text files and uploading to the target system, importing to a spreadsheet, etc. Further, proper validations and reconciliation of data is carried out between relevant interfaces/applications across the bank. The bank suitably integrates the systems and applications, as required, to enhance data integrity and reliability.

## **11. GENERAL INFORMATION REGARDING DELIVERY CHANNELS**

- Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking are issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. Customer is not being forced to opt for services in this regard. Bank provides clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.

- When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank ensure that the customers have sufficient instruction and information to be able to properly utilize them.
- To raise security awareness, Bank sensitizes customers on the need to protect their PINs, security tokens, personal details and other confidential data. Bank is responsible for the safety and soundness of the services and systems they provide to their customers. Reciprocally, it is also important that customers take appropriate security measures to protect their devices and computer systems and ensure that their integrity is not compromised when engaging in online banking. Customers implement the measures advised by their Bank regarding protecting their devices or computers which they use for accessing banking services.
- In view of the constant changes occurring in the internet environment and online delivery channels, management institute a risk monitoring and compliance regime on an ongoing basis to ascertain the performance and effectiveness of the risk management process. When risk parameters change, the risk process are updated and enhanced accordingly. Re-evaluation of past risk-control measures and equations, renewed testing and auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken are conducted.

## 12. CUSTOMER AWARENESS ON FRAUDS

### • CREATION OF CUSTOMER AWARENESS ON FRAUDS

1. Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Bank thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in Bank to create fraud risk awareness amongst their respective customers. The fraud risk management group shares its understanding of frauds with each group, identify areas where customer awareness is lacking and if required, guide the groups on program's to be run for creation of awareness amongst customers. The groups ensure that in each of their interaction with customers there is at least one message to make the customer aware of fraud risk.

2. The following are some of the recommended measures to create awareness amongst customers:

- Publications in leading newspapers
- Detailed 'do's and don'ts on the web site of the bank
- Messages along with statement of accounts, either physical or online
- Messages printed on bank's stationery such as envelopes, card covers, etc.

- 
- SMS /Email alerts for security tips (OTP/CVV/PIN/CARD/Transaction alerts Message) on phone banking when the customer calls
  - As inserts or on the jackets of cheque books
  - Posters in branches and ATM centres
  - Interstitials on television and radio

3. It is ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper precautions aimed at preventing frauds. Such communication is reviewed periodically by the fraud risk management group to judge its effectiveness.

## **13. EMPLOYEE AWARENESS AND TRAINING**

1. Employee awareness is crucial to fraud prevention. Training on fraud prevention practices are provided by the fraud risk management group at various forums.
2. Bank uses the following methods to create employee awareness:
  - Class room training programs at the time of induction or during risk related training sessions
  - Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank
  - E-learning module on fraud prevention
  - Online games based on fraud risks in specific products or processes
  - E-tests on prevention practices and controls
  - Detailed 'do's and don'ts' put up on the worksite of the employee
  - Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.
  - Emails sent by the respective business heads
  - Posters on various safety measures at the work place
  - Messages/discussions during daily work huddles

## **14. THREATS TO ATM NETWORKS**

As other networks, ATM networks will suffer a lot of threats. ATM threats/attacks can be divided into physical and logical attacks. Physical attacks involve attacking the ATM physically like exploding the ATM safe to have access to the ATM safe money. In physical attack, cyber criminals use methods such as solid and gas explosives, as well as uprooting the ATM from the site and then using other method to get access to safe and secure network. Other physical attack involves placing gadgets to ATM by cyber criminals that copy ATM card data and reproduce it on another blank card that can be used to perform unauthorized transaction from cardholder's account. Logical attacks include malware attacks to instruct ATM to perform the transaction. This attack can be achieved by gaining physical access on the ATM in order to install

---

malware on the system or it can be injected using network. Types of attacks on ATM network are as follows

- **ATM Card Skimming Attacks**

ATM card skimming attack is a physical threat which has been the number one ATM threat globally in the past. ATM skimming refers to the stealing of the electronic card data, aiding the criminal to counterfeit the card. A skimmer is a device that is installed on a card reader making a customer believe they are inserting their card in a ATM card reader. The skimmer reads the data from a card's magnetic stripe or EMV chip when a client inserts a card into the ATM. Some skimmers have the capability to read data from an EMV card chip at a distance. ATM skimming attacks are however, on the decrease due to deployment of anti-skimming solutions, payment card industry data security standard (PCI DSS), EMV technology and contactless ATM functionality. Customers are unable to notice a problem and experience a normal ATM transaction until their account is defrauded. The most common places where skimmers are placed on the ATM. Multifactor authentication using biometrics can be used as an added security mechanism against this type of fraud.

- **Eavesdropping Skimming Attack**

A new type of skimming attack called Eavesdropping Skimming has emerged and expanded predominantly in the world. The attack targets ATM motorized card readers on older model of ATM called personas. The attacker penetrates the ATM facial to have access to the card Reader of the ATM. A skimmer is then fitted directly onto an electrical node that carries card data on the card reader. On Personas ATMs, the attacker targets the card reader electronic control board by creating a hole behind the ATM card orientation window. In the newer attacks against ATMs, the attacker has changed the method but has maintained the principle. The variance in the way this attack is performed on the two different ATM series shows how sophisticated ATM cyber-criminals are.

- **ATM Card Shimming Attack**

ATM card shimming attack is a Man-in-the-Middle attack in which the cyber-criminal inserts a device into the ATM card reader that intercepts and records the data flowing between the EMV chip and the ATM card reader. This data could then possibly be reused to clone a magnetic stripe card. EMV chip data and magnetic stripe data have different check values (CVVs) and therefore the data that is captured from the EMV chip card can't be used to clone a magnetic stripe. Card Shimming is neither vulnerability with a chip card, nor with an ATM. It is therefore not necessary to add protection mechanisms against this form of attack to the ATM. If the proper authorization procedure is followed during an ATM transaction, counterfeit cards can be immediately detected. This attack can only be successful if an issuer neglects to check the CVV when authorizing a transaction. All issuers must therefore make these basic checks to prevent this category of fraud.

- **ATM Card Trapping Attack**

ATM Card Trapping steals the physical card itself through a device attached to the ATM. Cyber-criminals place a device directly over or into an ATM's card reader slot. These devices are designed to capture cards after customers' insert them. In a magnetic stripe environment or chip-and-signature environment, the PIN does not need to be compromised and therefore having an ATM is enough to compromise a Customer's account.

- **ATM Cash Trapping Attack**

Cash trapping is where the cyber-criminal uses a device to physically trap the cash that is dispensed and comes to collect it once the customer has left the ATM location. This fraud involves placement of money traps or false presenters in front of the ATM dispenser. When processing a transaction, an ATM dispenses notes into the trap set by cyber-criminals rather than present the money to the customer. The customer assumes the ATM has malfunctioned and leaves. The cyber-criminal then returns, removes the money trap or false presenter, and leaves with cash that was intended for the customer. Cash trapping however mostly succeeds with insider involvement. ATM owners must put measures in place that helps mitigate insider threats.

- **Transaction Reversal Fraud**

Transaction Reversal Fraud (TRF) involves the creation of an error that makes it appear as though the cash has not been dispensed. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction message. The attacker achieves this by creating a fault on the ATM during a cash dispense operation causing the host switch to reverse the transaction. The account will not be debited although the criminal will remove the cash from the ATM. To avoid being caught, attackers use stolen or skimmed cards. The attacker causes an error on the card reader during cash dispense operation. The correct PIN is entered and cash requested. After the transaction is authorized by the host switch, the ATM counts the cash and positions it behind the cash dispenser shutter waiting to be dispensed. The card is ejected and the attacker waits for the ATM transaction to time out and attempt to capture the card. At this point the attacker holds the card and prevents it from being captured and then forces the cash dispenser shutter open and removes the stacked cash. The ATM reports a card jam and reverses the transaction.

- **Social Engineering/Phishing Attacks**

The Victim is tricked into revealing his/her authentication information (PIN). It can be physically or through electronic means. e.g., rogue websites are set up by the perpetrators to collect authentication information from un-suspecting customers in the name of necessary updates or changes being carried out by their 'Bankers'. The user ends up divulging his card sensitive data to the rogue site.



---

- **Operational Fraud**

The ATM dispenser is manipulated in this type of fraud. The ATM is configured to dispense big denominations as smaller ones, thereby giving out more money than should be dispensed. This can be achieved by either loading wrong denomination notes in the wrong money cassettes or by making a wrong configuration in the software.

- **Malware Attacks**

Malware attacks are usually easier with insider involvement as physical access is necessary to deploy the virus. However, this attack is possible online today. The malware file or device is placed on the ATM; its control device is then triggered to give remote control to the perpetrator through a custom interface which enables capture of card numbers and PINs through the private memory space of transaction-processing applications installed on a compromised ATM. Magnetic stripe cards are very vulnerable to this type of attack. Deployment of effective anti-malware software can help mitigate this class of attacks.

- **Man-in-the-Middle Attack**

This class of attack occurs when malware is placed within the banks network and compromises the banks network infrastructure. The network traffic is monitored and the malware listens for transaction messages from the ATMs. When the malware recognizes a cash withdrawal transaction message from a bank Card, it intercepts the corresponding host response from the ATM switch and changes the authorized dispense amount to a larger sum than requested and approved by the ATM switch. In order to perform the fraud, an attacker will initiate a withdrawal transaction at any ATM on the compromised bank network. The attacker will use a pre-defined known card number. The transaction will be intercepted and the card number will be recognized by the malware. It will then wait for the host response to the withdrawal request. The malware will intercept the host response message and modify it to a larger amount therefore the ATM will dispense far more money than what is debited from the account. A variation of the attack, is where the malware intercepts the request, and returns an authorization message such that the transaction host is unaware of the request.

- **Ransom-ware Attacks**

A serious malware called “Wanna Cry” encrypts the files on end-points that are running Microsoft operating system software, rendering them inaccessible. The files are only decrypted upon payment of a sum of money known as ransom. This malware attempts to infect other end-points on the same network. The malware does not specifically target Banking and Retail systems or their functionalities but ATMs like any other Windows based system are also at risk of this attack. There have been unconfirmed media reports that some ATMs in India have experienced this attack. Prevention of infection via phishing emails by implementation of technical and organizational measures, Segment and secure local area Network (LAN)/ virtual

---

LAN (VLAN) with intrusion detection and prevention mechanisms to avoid infection and distribution of malware via the network,

- **ATM Jackpotting Attack**

The term ATM Jackpotting comes from the term Jackpot. In this type of attack, cyber-criminals get huge sums of money from the ATM at once. Cyber-criminals use two methods to perform this attack.

## 15. ATM INCIDENT MANAGEMENT POLICY AND PROCEDURES

The Bank has developed, communicated and implemented formal systems and procedures for detecting and reporting incidents relating to exceptional situations in day-to-day administration of IT and information security related areas. The Bank ensures that the incidents are reported in time to the appropriate authorities and corrective actions are taken immediately to provide the IT Service to Users as quickly as possible and to avoid the recurrence of such events in future

- **Definitions**

**“ATM” Automated** Teller Machine is a computerized machine that provides the customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions without the need of actually visiting a bank branch.

**“Incident”** is a term related to exceptional situations or any event which is not a part of the standard operation of a service and which causes or may cause an interruption to or a reduction in the quality of service or a situation that warrants intervention of senior management. An incident is detected in day to day operations and management of the IT function.

**“INCIDENT RESPONSE”** set of actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event or incident occurs; involves contingency planning and contingency response.

**“INCIDENT HANDLING”** Same as Incident Response.

**“INTRUSION”** any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them

**“CHAIN OF CUSTODY”** verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. For a proven chain of custody to occur, the evidence is accounted for at all times.

**“CONSTITUENCY”** Implicit in the purpose of a Computer Security Incident Response Team is the existence of a constituency. It is the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.

- **Responsibilities**

- ✓ Provide a (secure) channel for receiving reports about suspected incidents.
- ✓ Provide assistance to members of its constituency in handling these incidents.
- ✓ Disseminate incident-related information to its constituency and to other involved parties.

- **Procedures**

- ✓ Functions of IT Department with respect to Incident management
- ✓ The System administrators shall handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management
- ✓ Investigating whether indeed an incident occurred.
- ✓ Determining the extent of the incident.
- ✓ Incident Coordination
- ✓ Determining the initial cause of the incident (vulnerability exploited).
- ✓ Facilitating contact with other similar sites who have reported the incident (if applicable).
- ✓ Facilitating contact with appropriate law enforcement officials, if necessary.
- ✓ Making reports.
- ✓ Composing announcements to users, if applicable.
- ✓ Incident Resolution Removing the vulnerability.
- ✓ Securing the system from the effects of the incident.
- ✓ Evaluating whether certain actions are likely to reap results in proportion to their cost
- ✓ And risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc. Collecting evidence where criminal prosecution, or Disciplinary action, if contemplated.

---

- **Data Collection & Analysis**

- ✓ In addition, IT department will collect statistics concerning incidents which occur within or involve the bank's information resources, and will notify the relevant parties proactively as necessary to assist it in protecting against known attacks.
- ✓ The incidents noted are analyzed by the quality function on a semi-annual basis to identify trends, if any. A database containing following information for each incident noted is prepared for future use:

- **Type of Incident**

- ✓ Impact Analysis on the affected IT assets or business process
- ✓ Ways of detecting the incident
- ✓ Ways of resolution of incident
- ✓ Down time requirements
- ✓ Contact details for reporting and resolution Information Services: List of departmental security contacts, administrative and technical. These lists will be available to all users inside the bank and general public, via commonly available channels such as Intranet/World Wide Web.

- **Incident Handling & Management**

- i. Constituency**

An IT Department's constituency can be determined in any of several ways. For example, it could be a company's employees or its paid subscribers, or it could be defined in terms of a technological focus, such as the users of a particular operating system.

- ✓ The definition of the constituency should create a perimeter around the group to whom the team will provide service. The policy section of the document (see below) should explain how requests from outside this perimeter will be handled.

- ii. Detection and initial reporting:**

- ✓ An incident may be detected by anybody in the bank. The concerned personnel should immediately bring it to the notice of the person designated by IT department. The person so designated should escalate the issue as per escalation guidelines. The initial reporting covers following:
  - ✓ Time of the incident
  - ✓ Nature of the incident
  - ✓ Probable cause of the incident
  - ✓ Effect of the incident

- 
- ✓ Mode of resolution of the incident
  - ✓ Activity log in case the incident involves desktop / server / network operating systems or any of the applications.

### **iii. Documentation and formal reporting:**

- ✓ A person designated by departmental head should maintain the central database of all such incidents. The person so designated, after analysing the extent of exception and facts of the incident, should appraise the related IT department personnel. A detailed risk and impact analysis for the incident should be carried out by the IT team. (Refer to Annexure A, B for the formats of Incident management documentation).
- ✓ The IT department should ensure that all incidents are categorized based on the nature of each incident and are held in a database created for the purpose. The database should be able to provide information on demand and have the capability to perform analysis on the data contained within. The bank's employees encountering incidents would thus be able to access the incident database and possibly find solutions if the incident had occurred before. Frequently asked questions should also be incorporated into the database to assist the user in finding solutions to incidents encountered.

### **iv. Monitoring:**

- ✓ All the major incidents should be reviewed and monitored by the Security Administrator and discussed in the Technology Committee meeting every month. The magnitude and criticality of the incidents may prompt the System/Database / Network Administrators to discuss and take action on the incidents immediately instead of at fixed intervals.

### **v. Development of corrective action plan:**

- ✓ The IT department, in consultation with affected System administrator or any other person it deems fit should prepare the corrective action plan for the incident. The action plan, though specific to each case, should typically cover the following:
  - ✓ Facts and explanation / reasons for the incident
  - ✓ Corrective action to be taken
  - ✓ Estimated cost of implementing the corrective action
  - ✓ Estimated time frame, start date and end date
  - ✓ Personnel responsible for taking the action
  - ✓ Information exchange with other Incident Handling teams
- ✓ The IT department can share information with other incident management teams and general public with prior permission from Executive Director.

**Annexure A –Incident-Reporting Form**

Department:	Date:
Name of the employee:	Department:
Facts of the incident:	
Signature:	

**Annexure B Reporting of the incident to Level 2**

Department:	Date:
Incident reported by	Incident occurred on:
Facts of the incident.	
Analysis of the incident by Head of Department and impact:	
Signature:  Systems Administrator / Operator in charge of the branch	Signature:  Head

---

## 16. ATM CUM DEBIT CARD ACCEPTANCE OF USE POLICY

### Policy for governing the Bank Debit card (ATM-CUM-DEBIT CARD)

#### Definitions:

The “Member Bank” refers to The Muslim Co-operative Bank Ltd. ,

The “Sub member Bank” refers to The Muslim Co-operative Bank Ltd. The Bank, our, us or we refers to Sub member Bank that is The Muslim Co-operative Bank Ltd. a body corporate constituted under the Maharashtra Co- Operative Society Act (Acquisition and Transfer of Undertaking) Act 1960 having its Registered Office which expression shall mean and include its successors and assigns.

**XXXX Switch**, is application service provider.

**Cardholder**, you, your refers to a customer of the Bank, who has been issued and authorized to use The Muslim Co-operative Bank Ltd. Debit Card.

The issuer in relation to cardholder means the Bank.

**The card** means The Muslim Co-operative Bank Ltd. Debit Card” issued by the issuer to Cardholder.

**Account** in relation to Debit Card means an account opened and maintained by The Muslim Co-operative Bank Ltd. for the purpose of routing card related transactions under this agreement, which also includes an account of a customer of the Bank who has agreed to these terms and conditions and is authorized to operate the Bank account and thereby use the banking Services including ATM services and includes those having joint accounts, Multiple users.

Customer includes any individual, sole proprietorship firm, partnership, company, co-operative society, association and corporation, association of persons, trust or other legal or natural entity or organization.

**ATM** means any Automated Teller Machine in India whether of the Bank or a shared network ATM located displaying RUPAY logo, which honours the Debit Card.

A **PIN** means the personal Identification Number (required to access ATMs) allotted to the Cardholder by the Bank or chosen by the cardholder from time to time.

---

**Charges** shall mean all amounts charged to the account under this terms including but not limited to purchase of goods, services or cash by use of the Card, joining fee, annual fees, interest charges, finance charges, transaction charges, service charges and any taxes, applicable from time to time.

**Merchant** or Merchant Establishment shall mean any company, establishment, and/or person wherever located, which a RUPAY Card Scheme Member Bank has approved and made arrangements with, to accept and honour the card, for the sale of goods and service to Cardholders. This shall include among others, stores, shops, restaurants, airline organizations etc. advertised by the **BANK or RUPAY.**

**“BM”** means Branch Manager.

**\*NPCI**” stands for National Payment Corporation of India

**“EDC’** or “Electronic Data Capture”, refers to Electronic Point-of-sale swipe terminals, whether displayed by or on behalf of Bank or any other Bank at which, amongst other things, the cardholder can use his fund in his account(s) held with the Bank to process the transaction at a Merchant Establishment. Transaction” means any instruction given, by a cardholder by using his card, to the Bank to effect action on the account. (Examples of transactions can be retail purchases, cash withdrawals, etc.)

#### **The CARD:**

The Muslim Co-operative Bank Ltd. Debit Card shall be issued on the basis of an application in the prescribed format subject to such eligibility norms the issuer may fix from time to time. The issuer at its sole discretion may refuse issuance or renewal of card without assigning any reason whatsoever.

The cardholder shall be deemed to have unconditionally agreed to be bound by the

Terms and conditions by acknowledging receipt of the card in writing or by signing on the reverse of the card or by incurring a charge on the card. However, the account holder may refuse to be issued a card subsequent to have applied but has not accepted for whatsoever reasons. In such cases, if the card is already received by the branch of issue, the card shall be destroyed by cutting into two pieces. No refunds shall be made of the charges for the card, which were ordered and subsequently refused.

The Muslim Co-operative Bank Ltd. Debit Card is valid only in India. The card is valid up to the last day of the month of year Indicated on the face of the card unless cancelled /invalidated earlier. On expiry/earlier cancellation/ invalidation, the Card must be destroyed by cutting into two pieces and shall be returned to the issuer.

A Membership renewal fee will be charged at the time of renewal of cards on expiry.



Annual fee at the prevailing rate will be levied at the time of issuance of the card which will be collected by debiting to the account for each of the card issued to the account and then annually during the month in which the card was originally issued. The fees are subject to revision by the Bank from time to time.

The Cardholder will be responsible for all facilities granted by the Bank in respect of the card and for all related charges. A tariff of charges has been given elsewhere in this document, which is subject to changes from time to time. The Card along with the acknowledgment issued will be sent to the Branch who had forwarded the application.

The applicant shall sign the acknowledgment and return it to the branch for having received the Card/s. The Cardholder shall sign on the reverse of the Card immediately on its receipt and shall take all reasonable care for its safe custody. The Card holders shall also note down the Card Number and validity period, as imprinted on the Card, separately to enable him/her to furnish these details to the issuer in case of loss or theft of the Card as required in terms of Para.05 hereof. The renewal Card along with acknowledgment will be dispatched by the Issuer to the Branch where the Cardholder maintains his/her account.

The Card is a property of the Bank and the issuer reserves its right to cancel the Card and/or withdraw the privileges extended to the Cardholder under the Card at any time without assigning any reason. The issuer shall have absolute right to retrieve the cancelled/withdrawn Card and must be surrendered to an authorized person of the Bank on Demand. The cardholder shall ensure that the identity of the authorized person of the Bank is established before handing over the card. Continued possession and/or use of such card by the Cardholder would constitute an illegal act exposing the Cardholder to legal proceedings.

The issuer may at its Sole discretion and without the Cardholder having to make specific request to renew, renew the Card whose validity has expired or is going to expire, for a further period presently of 5 years unless the Cardholder specifically indicates his wish to the contrary (Informing at least 2 months in advance of the expiry period). And upon such renewal all the terms and conditions hereof shall apply to such renewed card. The Bank will initially allocate a Personal Identification Number (PIN) to the cardholder. The cardholder may select his own PIN (any 4 digit number) if he would like to change it, depending on the availability of such facility in our ATM. The PIN issued to the cardholder for use with the Card or any number chosen by the cardholder as a PIN, will be known only to the cardholder and to the personal use of the cardholder and are non-transferable and strictly confidential. A written record of the PIN should not be kept in any form, place or manner that may facilitate its use by a third party. The PIN should not be disclosed to any third party, under any circumstances or by any means whether voluntary or otherwise. The cardholder shall be

liable for any damages arising from a failure to keep secrecy of the PIN. In case the cardholder already has The Muslim Co-operative Bank Ltd. ATM card, on his acceptance/deemed acceptance of the Debit card, the ATM card issued to him, (if any) will be cancelled/deactivated by the Bank subsequently.

**Use of the CARD**

The Cardholder must not permit any other Person to use the Card and should safeguard it from misuse by retaining it under his/her personal custody at all times. The Cardholder's account will be debited immediately with the amount of any withdrawal, transfer and other transactions effected by the use of the card. The cardholder will maintain sufficient funds in the account to meet any such transactions and shall not be entitled to overdraw the account(s) with the Bank or withdraw/purchase by the use of the Debit Card in excess of any agreed overdraft limit. In case of cards linked to multiple accounts, transactions at ATMs (where account selection option is not available), Merchant Establishments and Cash withdrawals through EDCs will be affected on the primary account linked to the card. In case there are no funds in this account, the Bank will not honour The transactions even if there are funds available cumulatively or severally in other accounts linked to the same card.

The **Bank and RUPAY** Card shall not be liable when a merchant for any reason refuses to accept the Debit card or the ATM/EDC has not rendered the requested service of the Debit card cannot be used as a result of any defect, blocking, deactivation, temporary insufficiency of cash in the ATM, technical or communication failure.

**Merchant Location Usage (POS Transaction)**

The card is acceptable at all electronic Point-of-sale across the Globe which display the **RUPAY** Card Logo. The card is for electronic use only and will be accepted only at Merchant Establishments that have an electronic Point-of-sale swipe terminal. Any usage of the card other than electronic use will be deemed unauthorized and Cardholder will be solely responsible for such transactions. The card is operable with the help of the cardholders signature or the PIN at EDC terminals installed at Merchant Locations depending on the functionality of the EDC terminal. Use of the Card at Member Establishment will be limited by the limit assigned for all such transactions for a day, irrespective of the credit balance in the account(s). Transactions are deemed authorized and completed once the EDC terminal generates a sales slip. The amount of the transaction is debited from the primary account linked to the card immediately. The cardholder should ensure that card is used only once at the Merchant Location for every purchase. The sales slip will be printed each time the card is used and the cardholder should ensure that there is no multiple usage of card at the Merchant Location at the time of purchase. Authority to charge the Cardholder's account in respect of purchases made/to be made services availed/to be availed would be given by Cardholder's either in the form of charge slip or such other form as the Bank may prescribe. Signature of the Cardholder on such form/form together with the Card No. Noted thereon or

any sales slip not personally signed by the cardholder, but which can be proved, as being authorized by the cardholder, shall be conclusive evidence as between the issuer and the Cardholder as to the extent of liability Incurred by the Cardholder and the Issuer shall not be required to ensure that the Cardholder has duly received the goods purchased /to be purchased or has duly received the services availed/to be availed up to his/her satisfaction.

The Bank accepts no responsibility for any surcharge levied by any merchant establishment and such amount will be debited to the cardholder's account. However, some transactions (like at Railway Stations & Petrol pumps) may attract a service charge as per the Industry practice in addition to the Amount of transaction which will be debited to cardholder's account. The Cardholder must retain his own copy of the charge slips. Copies of charge slips will not normally be provided by the Bank/ issuer. However at its discretion and upon customer request, the Bank/Issuer may provide copies thereof if request is received in writing within 15 days from the date of transaction, subject to an additional fee, which charge is subject to change at the discretion of the Bank/Issuer. The card is not to be used at Hotels during check-in and also at other locations where paying arrangement is done before completion of the purchase transaction or service. The card should not be used for any Mail Order/Phone order / purchases and any such usage will be considered as unauthorized. Should the Cardholder choose to disagree with amount debited to his account, the same should be communicated to the Bank/Issuer within 15 days of the transaction date, failing which it would be construed that all charges are in order. The Bank/Issuer is not responsible or liable for any defect or Deficiency in respect of goods and services charged to the Card. Any dispute should be settled directly by the Cardholder with the Member Establishment and failure to do so will not relieve the Cardholder of any obligations to the Bank/Issuer. No claim by the Cardholder against a Member Establishment will be a subject, set off, or counterclaim against the Bank/Issuer. Any purchase/ailment of service and subsequent cancellation thereof (including purchase and cancellation airline/railway Tickets, etc) shall be treated as two different transactions. On receipt of refund/credit if routed through the Issuer, the actual net amount so received shall be held by the Issuer on behalf of the Cardholder free of Interest and settled against the claim made by the cardholder by crediting to the account subject to recovery of a service charge as may be fixed from time to time. The claim should be supported by some proof like cancelled charge slip copy, refund vouchers etc. All refunds and adjustments due to any merchant/device error or communication link will be processed manually and the account will be credited after due verification and in accordance with **RUPAY** rules and regulations as applicable. The cardholder agrees that any debits received during this time will be honoured only based on the available balance in the Account (s) without considering this refund/adjustment. The cardholder also indemnifies the Bank from such acts of dishonouring the payment instructions.

The cardholder shall make use of the Card only for making bona-fide purchase of goods or ailment of services from such Member Establishments with whom the Bank may enter into

arrangement for this purpose, or such Merchant Establishments who are authorized to accept Cards with RUPAY Card logo or for making "Cash Withdrawal" as indicated in clause 04 hereof, Within the validity period of the Card. The Cardholder shall not, while making use of the Card commits any breach or violation of any law, rule or regulation that may be currently in force. The Issuer reserves the right to call for from the Cardholder and/or the Member Establishment full details of the transactions under the card, and the Cardholder shall agree to such disclosure. The Cardholder alone shall make use of the Card and shall not allow any other person to use the same on his/her/its behalf. The Card shall not be transferable.

The bank reserves the right and the cardholder agrees inter alia for the disclosure and share and receive from other institutions, credit referencing bureaus, agencies, statutory executive, judicial and regulatory authorities whether on request or under an order there from, and on such terms and conditions as may be deemed fit by the Bank or otherwise, such information concerning the cardholder's account as may be necessary or appropriate in connection with its participation in any Electronic Funds Transfer network. The bank also reserves the right of disclosure of information to third parties about the bank account of the cardholder or the transactions done through the use of the card where it is so necessary for completing transactions and/or when necessary to comply with law or government agency or court orders or legal proceedings and/or when necessary to resolve errors or to resolve other matters. Any government charges, duty or debits, or tax payable as a result of the use of the card shall be borne by the cardholders and if imposed upon the Bank (either directly or indirectly), the Bank shall debit such charges, duty or tax to the cardholders account,

#### **CASH WITHDRAWALS:**

The card is accepted at any of The Muslim Co-operative Bank Ltd. ATMs (Cash Points) and other bank ATMs/ displaying Rupay Card logo. The card is operable with the help of a confidential PIN at ATM locations. On receipt of the PIN by the cardholder from the Bank/issuer, he should ensure that the same is received in a sealed envelope and that there are no signs of tampering of either the envelope or the PIN mailer. All transactions conducted with use of the PIN will be the cardholder's responsibility and he will abide by the record of the transaction as generated.

The Cardholder may avail cash withdrawal in Indian Rupees with a minimum of Rs. 1xx or its equivalent and subject to a maximum of Rs. 2500xx per day in multiples of Rs. 1xx or any such amount as may be notified by the Issuer from time to time.

When the card is used at any other shared ATM, the bank will not accept responsibility for any dealings the cardholder may have with the other institutions including but not limited to such services. Should the cardholder have any complaints concerning any shared network ATM establishment, the matter should be resolved by the cardholder with the establishment

and failure to do so will not relieve him from any obligations to the Bank. However, the cardholder should notify the bank of this complaint immediately.

There will be separate service charges levied for such facilities that will be fixed by the Bank from time to time and debited to the cardholder's account linked to the card at the time of making such transactions.

In the situation that the account does not have sufficient funds to debit such fees, the Bank reserves the right to deny the transaction. And the decision of the Bank is binding on the cardholder. Such service charges will be debited to the account irrespective of the fact that a transaction is successful or is a failed one. The type of transactions offered on shared network ATMs may differ from those offered on the Bank's own network. The bank will only support the minimum transaction set that will be offered at the ATMs belonging to other networks. The Bank reserves the right to change the transaction set without any notice to the Cardholder.

For all cash withdrawals at The Muslim Co-operative Bank Ltd. ATM, any statements/receipts issued by the ATM at the time of withdrawal shall be deemed conclusive, unless verified and intimated otherwise by the Bank. Any such verification shall likewise be final and conclusive and this verified amount will be binding on the Cardholder.

### **LOST OR STOLEN CARD**

If the Card is lost / stolen, the Cardholder shall immediately notify the branch (which has issued the card)/nearest branch /Switch room with full details, including the Cardholder's name, the Card Number and its validity period as imprinted on the Card. If this information is given orally, it must be confirmed in writing within 7 days. The Cardholder shall furnish to the Issuer all information in his/her possession as to the circumstances of loss/theft and take all reasonable steps, such as informing the issuer by quick mode of communication, lodge a complaint with local police etc. to recover the lost/stolen Card and shall also assist the Issuer to recover it. In case of suspected theft of a Card, the Cardholder has to lodge a report with the local police and has to send a copy thereof to the issuer. Subject to compliance by the Cardholder, with these requirements, the Cardholder's liability arising as a result of any other person unauthorized using lost/stolen Card for purchase transactions after the receipt by the issuer (branch of issue) of information of loss/theft of the Card will be ZERO. However there will be no such coverage provided on cash withdrawals done through ATMs, as such transactions require the use of a PIN, which is confidential to the cardholder. In case the Cardholder recovers the card which was reported as lost/stolen, he/she shall not make any further use of it and it shall be surrendered to the issuer along with a full report giving the details of its recovery. The Cardholder will be fully liable for all the charges on the Card in the event that it is lost but not reported in writing as above to the Bank/Issuer and the Cardholder hereby indemnifies the Bank/ Issuer fully against any liability (civil/criminal) loss, cost, expenses or damages that may arise due to loss or misuse of the Card. In the event the

transactions are received by the Bank/Issuer after the Card has been reported lost or stolen but before the receipt of the Cardholder's written confirmation and police complaint/FIR as above, the Cardholder shall continue to be fully liable for all amounts debited to the cardholder's account. A fee of Rs 150 per Card or such other amount as may be fixed by the Bank from time to time shall be charged from the Cardholder for placing the lost/stolen Card in the Hot List, This fee has to be paid compulsorily whether the lost/stolen Card is to be replaced or not.

### **PRICING STRUCTURE: (CHARGES / FEES)**

#### ATM Use Charges

1. Membership Fee:
2. Activation Fee: Free.
3. Annual Maintenance Fees: Rs. 236.
4. Hotlist/Duplicate card because of loss of card: Rs. 236.
5. Replacement card: Rs. 236
6. Transaction charges at The Muslim Co-operative Bank Ltd. ATMs: NIL.
7. Transaction charges at other Bank ATMs: It varies from Rs. 15 to Rs. 25 per transaction.
8. Balance enquiry at other bank. ATMs: Rs. 10 per occasion limits.

#### POS Use Charges

1. Per Day POS transactions at Merchant Establishments: Rs. 2, 00,000.
2. per Day ATM Cash Withdrawal: Rs. 20,000.00. In addition to above service tax if applicable and at applicable rates from time to time will also be charged. The fees/charges/Limits indicated here are as prevalent currently and are subject to revision by the Bank from time to time. Annual Fee / Renewal 'Fee will be collected in advance. First collection of the Annual fee will be starting of new financial Year (i.e. linking by the branch) and subsequent collections on the 1st day of the corresponding month of issue of each year.

### **GENERAL CONDITIONS:**

The Cardholder shall undertake to furnish to the Issuer, changes, if any in respect of any information furnished in the application form within 7 days from the date of occurrence of such changes. The Issuer may take cognizance of such changes only after the expiry of 30 days from the date it duly receives the information. All suits and proceedings against the Issuer relating to any claims, dispute or differences arising out of or in respect of the Card shall be instituted only in the courts situated in the city of **Bangalore** where the Head Office of the Issuer is situated and no court/forum situated in any other place shall have jurisdiction to entertain or decide such matters the Issuer may, however at its option institute any such suit or proceedings against the Cardholder at any place where the Cardholder resides or carries on business or works for gain or maintains his/ her/ its account with any branch of the Issuer. The Issuer reserves their right to add to, delete from these

Terms and Conditions as they think fit in their absolute discretion and without assigning any reason whatsoever and such changes shall be binding on the Cardholder.

### **Guideline Policy for General User**

The debit card is valid for use in INDIA and member of NPCI Banks ATM only. The card is valid for a period of 5 years, valid from the date of issue till the last day of the month of expiry.

Verify whether your name is imprinted correctly on the face of the card. If not, take up the matter with your branch of issue. Sign across signature panel at the back of your card, to prevent misuse of the card. Collect the PIN mailer from the branch and ensure that the PIN number is not tampered. If any signs of tampering is found, immediately surrender the card & PIN to the branch of issue. Protect your card and do not Give access to any one to have your card. Bend or scratch the card as damage will be caused to the magnetic stripe on the reverse of the card which contains important information about the card. Before due date the card will be automatically renewed and sent to your branch from whom you may collect and continue to use the card. If you do not wish to renew the card, for any reason, the branch of issue has to be intimated at least 2 months in advance. If the renewed card has not been received by you within the expiry date of the earlier card, please do take up with the branch immediately.

### **USAGE AT MERCHANT OUTLETS:**

The Muslim Co-operative Bank Ltd. Debit Cards affiliated to RUPAY are accepted at all Merchant Establishments displaying RUPAY Logo. The Merchant should have an electronic (Point- of- sale) swipe terminal. Usage is permitted up to Rs. 50,000 per day at Merchant locations say, Restaurants, Hospitals, Departmental Stores, Textile outlets, Jewelleries etc. Present your debit card for payment of the purchase amount. The merchant will swipe the card in the point-of-sale machine for authorization. After a successful authorization, a charge slip is generated from the POS machine. Ensure for correctness of the amount and sign the charge slip exactly as appearing on the reverse of your card. Collect back your card and your copy of the charge slip. Please retain the charge slip copy till you verify the amount as appearing in your bank statement of account.

There are certain exceptional cases where you may be billed extra service charges while making use of your Card with MEs such as Petrol Bunks, Railways, etc. Only if you agree to bear extra charges, you should proceed with the transaction. Such service charges together with the charge slip amount will be debited to your operative account.

Please note that since signature verification is essential for debit card transactions you need to be physically present along with your card at the time of purchase.



**ATM:**

Your DEBIT-CARD is linked with ATMs (Automated Teller Machines) for easy access to the cash, 24 hours a day. Your DEBIT CARD is accepted not only at The Muslim Co-operative Bank Ltd. ATMs but also at all ATMs of other banks which are member with NPCI. Instructions for operations in ATMs: The ATM Cash Withdrawal limit is Rs. 20,000 per day. Please insert the card in the top right corner in the Card Insert slot. Then the machine will respond to you with the message "Enter your PIN No'.

Key in your PIN No. within 15 seconds and follow the instructions given on the screen.

**IMPORTANT:**

Please collect the card from the ATM and also the cash immediately; else the ATM will swallow the card/cash as the case may be. Other services, offered at our ATMs are:

- (1) Cash withdrawal
- (2) Balance enquiry
- (3) Mini Statement
- (4) Request for cheque book
- (5) Statement request,
- (6) PIN change.

**Note:**

For any ATM operational assistance/clarifications contact the Branch Manager or the ATM officer in charge of ATM switch room. **Customer Care PHONE NO. 02482/233346**

**DISPUTE:**

As the transactions are debited on line, any dispute relating to a transaction should be reported to the branch of issue of card within 15 days from the date of transaction. The branch in turn will take up with Card Division regarding the transaction disputed who will take steps for resolving the dispute.

**SAFE CUSTODY:**

Please preserve your The Muslim Co-operative Bank Ltd. ,DEBIT CARD carefully and do not let it fall into wrong hands. Please check your wallet/pouch once in a while and ensure that your card is always safe.

Despite the above, if you lose your The Muslim Co-operative Bank Ltd. , DEBIT CARD, please inform the same to your Branch/Switch room your Name, Card Number & Validity so that the card can be hot listed. Simultaneously, please lodge a police complaint immediately detailing the loss. A copy of the police complaint along with your detailed letter confirming the loss should be sent to the branch of issue within a week from the date of reporting the loss. Fresh letter of request should be given to the branch for issue of New DEBIT CARD. Please avoid loss on account of someone misusing the lost/stolen card by promptly reporting



---

the loss of the card for hot listing. If you trace the lost card after reporting the card loss, please do not use it, since it will not be honoured by the MEs (Merchant Establishment)/branches. Please destroy the card beyond use and confirm the Branch of issue of the card.

**Terms and Condition:-**

By accepting and/or using the card / signing on the reverse of the Debit Card the cardholder accepts the terms and conditions set out for The Muslim Co-operative Bank Ltd. debit Card unconditionally and will be bound by them and accepts the onus of ensuring compliance with the relevant Reserve Bank of India (RBI) regulations, Exchange control Regulations, Foreign Exchange Management Act and any other corresponding enactment in force from time to time. The cardholder will also continue to remain bound by the terms and conditions of operations of his Savings Bank Account/ OD Accounts/ Current Accounts with The Muslim Co-operative Bank Ltd. These terms and conditions shall be known as "The Muslim Co-operative Bank Ltd. ,Debit Card rules and shall have come into effect immediately.

## 17. FAQs FOR ATM DEBIT/CREDIT CARDS

**Automated Teller Machine (ATM)?**

Automated Teller Machine is a computerized machine that provides the customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions without the need of actually visiting a bank branch.

**What Type Of Cards Can Be Used At An ATM?**

The ATM cards/debit cards, credit cards and prepaid cards (that permit cash withdrawal) can be used at ATMs for various transactions.

**What Are The Services / Facilities Available At ATMs?**

In addition to cash dispensing ATMs may have many services / facilities such as:  
Account information

- Regular bills payment
- Purchase of Re-load Vouchers for Mobiles
- Mini/ Short Statement

**How Can One Transact At An ATM?**

For transacting at an ATM, the customer insert (swipe) their card in the ATM and enter their Personal Identification Number (PIN).

**Can These Cards Be Used At Any Bank ATM In The Country?**

Yes. The cards issued by banks in India should be enabled for use at any bank ATM within India.

**What Is A Personal Identification Number (PIN)?**

PIN is the numeric password for use at the ATM. The PIN is separately mailed / handed over to the customer by the bank while issuing the card. This PIN has to be reset to a new PIN by the customer. Most banks force the customers to change the PIN on the first use. The PIN number should not be written the card, card holder etc. as in such cases the card can be misused if card is lost / stolen.

**What Should One Do If He Forgets PIN Or The Card Is Sucked In By The ATM?**

The customer may contact the card issuing bank branch and apply for retrieval/issuance of a new card. This procedure is applicable even if the card is sucked in at another bank's ATM.

**What Should Be Done If The Card Is Lost / Stolen?**

The customer may contact the card issuing Branch immediately on noticing the loss so as to enable the bank to block such cards.

**Is There Any Minimum and Maximum Cash Withdrawal Limit per Day?**

Yes, banks set limit for cash withdrawal by customers. The cash withdrawal limit for use at the ATM of the issuing bank is set by the bank during the issuance of the card. This limit is displayed at the respective ATM locations. For cash withdrawals at other bank ATMs, banks have decided to maintain a limit of Rs 10,000/- per transaction. This information is displayed at the ATM location.

**Do Banks Levy Any Service Charge For Use Of Other Bank ATMs?**

No charges are payable for using other banks' ATM for cash withdrawal and balance enquiry, as RBI has made it free under its "Free ATM access policy" since April 01, 2009. But banks can restrict the number of such free transactions to a maximum of five per month. For transactions beyond this minimum number of transaction, banks charge maximum of Rs 20/- + GST per transaction.

---

**What Should Be Done In Case During The Cash Withdrawal Process, Cash Is Not Disbursed By The Account Gets Debited For The Amount?**

The customer may lodge a complaint with the card issuing bank. This process is applicable even if the transaction was carried out at another banks ATM.

**How Many Days Maximum Would The Bank Require To Re-Credit The Account For Such Wrong Debits?**

As per the RBI instructions, banks may re-credit such wrongly debited amounts within a maximum period of 12 working days.

**Is The Customers Eligible For Compensation For Delays Beyond 12 Working Days?**

Yes. Effective from July 17, 2009, banks shall have to pay customers Rs. 100/- per day for delays beyond 12 working days. This shall have to be credited to the account of the customer without any claim being made by the customer.

**In Case The Compensation Is Not Credited As Mandated, What Recourse Does The Customer Have?**

For all such complaints customer may lodge a complaint with the local Banking Ombudsman if the bank does not respond.

**What is a The Muslim Co-operative Bank Ltd. Bank Debit Card?**

The Muslim Co-operative Bank Ltd. Bank Debit Card is a plastic card, which provides access to ATMs for cash Withdrawals, balance enquiries and mini statement. It also provides on-line electronic payment for purchases from your savings / current (individual) accounts.

**What are the variants of The Muslim Co-operative Bank Ltd. Debit Card?**

The Muslim Co-operative Bank Ltd. ,Debit Card – Classic

**Whether Debit Cards can be issued in Joint accounts with operation condition “Jointly “?**

Yes. The Debit Cards can be issued to 2 Signatories in Joint Accounts with operation condition jointly. Joint operation in ATMs using two cards with two distinct PINs, for withdrawal of cash, in case of Joint Accounts with operation condition “Jointly” and having only two joint holders, is available. However, such cards shall be issued at specific request of the Account Holder and shall be used only for Cash withdrawal in our bank ATM’s only.

**What is PIN (Personal Identification Number)?**

- ❖ PIN is a unique 4 digit number that allows you to access your account through Debit
- ❖ Card at ATMs.

- 
- ❖ Please keep your PIN safe.
  - ❖ Please memorize the PIN.
  - ❖ Do not write the same on any material, which is accessible to unauthorized persons.
  - ❖ Do not divulge the PIN to anybody, even to Banks' personnel.
  - ❖ Do not keep the PIN and the Debit Card together.

### **How can I get a Debit Card?**

Debit card can be obtained from the branch of The Muslim Co-operative Bank Ltd. where you maintain the account by filling a Debit Card application form. In case of Non-Personalized card (Without name) the card would be issued instantly. In case of personalized card (with name) the card would be issued within 7-8 working days

### **I have not received my personalized card even after 10 days of giving the request at the branch?**

Please contact the branch. You will get an SMS on your registered mobile number on dispatch of the Card to your branch.

### **I have received the Debit Card but the PIN is not legible.**

You should contact the card issuing branch and request for issue of replacement Card. Please destroy the old card. Bank will not preserve the PIN number and hence no reprint of the PIN is possible. PIN has to be generated afresh for the card. You can collect the replacement card & PIN from the branch after 15 working days.

### **Where my Debit card can be used?**

Debit Card can be used on all the ATMs & merchant establishments displaying Visa/MasterCard/RuPay logo. You can also use your card for payments on the Internet. Debit card issued will be of Domestic validity. On specific request Debit cards with global validity will be issued.

### **How does the Debit Card work?**

Insert your Debit card in ATM and follow the instructions displayed on the screen. On POS you need to swipe the card and sign the Bill after verifying the amount.

### **What is the validity of The Muslim Co-operative Bank Ltd. Bank Debit Card?**

Validity of Debit cards are till the last day of the month shown under "valid thro' on the face of the card.

### **Are there any transaction limits for the Debit Card?**

For The Muslim Co-operative Bank Ltd. Bank Debit Card — Classic the Cash Withdrawal at ATMs is limited to Rs. 30,000 per day and for purchase transaction Rs. 50,000 per day

**If Debit card is lost or misplaced, what should I do?**

Please call xxxxx get the card hot listed / blocked. Also inform the Branch where the card is issued, for blocking the card. The Muslim Co-operative Bank Ltd. Bank Debit Card can be hot-listed / blocked by using Banks mobile Banking Application.

**Is there any Fee for the issuance of Debit card?**

Debit Card Cost:- 200 + GST (AMC will be free for First Year). An Annual Maintenance fee of Rs. 200 + GST is applicable for The Muslim Co-operative Bank Ltd. Bank Debit Cards - Standard from the second year onwards. Annual fee will be collected on last month of financial Year and every year till expiry of the card.

**Is there any charge levied for use of the card for Cash withdrawal?**

No charge is levied for use of the card for cash withdrawal at The Muslim Co-operative Bank Ltd. Bank ATMs. For cash withdrawals at other Bank ATMs, please refer to "Service Charges" Section in our Home Page.

**Can a fresh Debit card be issued in lieu of lost/damaged card and what is the amount to be charged?**

Cards damaged due to wear and tear will be replaced free of cost. Cards issued in replacement of lost card will be charged Rs. 200 + GST/-.

**If lost card is subsequently found/traced and restored to cardholder, can it be reactivated?**

Card once hot listed / blocked cannot be re-activated. You can make a request for issue of a fresh card.

**What is Mini Statement?**

It is a statement of account showing last 10 transactions made in the account.

**How should I maintain the secrecy of PIN?**

If at any time you feel that the PIN has been inadvertently or otherwise divulged to any one, you should change the PIN through any The Muslim Co-operative Bank Ltd. Bank ATM immediately.

**How often can I change the PIN?**

PIN can be changed any number of times.

**How many accounts maximum can be linked to my Debit card?**

Only one account can be linked to a Debit card.

**Does Bank bear any liability for unauthorized use of the Card?**

No. The responsibility is solely vested with the cardholder.

**What is CVV No.?**

---

---

On the back of Debit card (Classic) there are 7 digits out of which the last 3 digits are the card CVV no. This number can be used only for transactions on the Internet.

**What is Add-On card facility?**

There is no Add on Card facility for The Muslim Co-operative Bank Ltd. Bank Debit Cardholders.

**Whether PAN is compulsory for applying for Debit card?**

Yes. PAN is compulsory as per RBI guidelines. Wherever PAN is not available, form No.60/61 as applicable has to be submitted.

**Whether Debit card can be issued to joint accounts?**

Debit card can be issued to joint accountholders where the operation condition is “severally”.

**My Debit card doesn't work successfully on ATMs?**

Debit Card does not work successfully on ATMs due to any of the following reasons;

- You may be using the card before the expiry of 3 working days of receipt of the card from the branch, the time required for activation of the card.
- You may not have swiped the card properly. Try 2 to 3 times.
- The magnetic stripe of your card has been damaged / deteriorated, due to which it is not accepted by any ATM where the card reader may be weak. In such a case, you may try at another nearby ATM and if still does not work, get it replaced by a new one from the Card-issuing branch free of cost.
- Your account may be inoperative or frozen at branch level due to some reason.

Please contact your branch to know the account status.


- You may be using wrong PIN.
- You might have selected the wrong account type i.e. savings instead of current or vice-versa.
- Connectivity from the ATM to your branch has failed. In such case please try after some time or use another ATM nearby.

**My Debit card works successfully on The Muslim Co-operative Bank Ltd. Bank ATMs but not on other Bank's ATMs.**

The problem may be due to connectivity failure at other bank ATM. Please try after some time when connectivity is restored. Alternately, you may try another ATM nearby.

**My Debit card works successfully on ATMs but not at POS terminals.**

Debit card does not work successfully on POS terminals due to any of the following reasons;

-  Connectivity failure at that particular time.

---

✚ Weak card reader of POS.

✚ Magnetic stripe of the card deteriorated / damaged.

You may use the card after some time when the connectivity is restored. Where the magnetic strip is damaged, you may obtain replacement card through your branch of issue, free of cost.

**My card doesn't work on few ATMs of The Muslim Co-operative Bank Ltd.**

The quality of the magnetic stripe of your card may be damaged / deteriorated, due to which it is not accepted by few ATMs where the card reader may also be weak. Try at some other nearby ATM. In such case you may get the card replaced by a new one through your The Muslim Co-operative Bank Ltd. ,Bank branch, free of cost

**What is the Insurance cover available for RuPay Debit card?**

NPCI offers accident Insurance of Rs. 1 Lakh for RuPay card. The Insurance is available till ATM card in service.

## 18. ROLES AND RESPONSIBILITIES

The Administrative Management is responsible for approval and execution of the ATM Policy. The policy shall review on yearly basis.

## 19. INQUIRIES

Inquiries regarding this policy can be directed to the Head of Information Security/CEO.

## 20. AMENDMENTS (REVISION HISTORY)

Amendments to this policy will be published from time to time and circulated to the

Post-Implementation Policy Review: Annually

## 21. DOCUMENT HISTORY

As per the version control sheet

\*\*\* End of Document \*\*\*